

In the Claims

The status of claims in the case is as follows:

1 1. [Currently amended] Method for nesting IP Sec-based
2 VPN connections between a plurality of nodes in a
3 communication network in which nested connections establish
4 a tunnel within a tunnel including an inner connection and
5 an outer connection having at least one coincident endpoint
6 residing on a same node, comprising the steps of:

7 receiving at a first node ~~on an~~ on said outer
8 connection a request from a second node to establish a
9 coincident endpoint for nesting ~~an inner~~ a secure inner
10 connection within said outer connection;

11 negotiating over said outer connection parameters
12 defining said inner connection and resulting from
13 Internet key exchange (IKE) negotiations for
14 establishing an agreed upon encryption algorithm and
15 key generation; and thereafter

16 responsive to communication occurring on said inner
17 connection, at said first node linking said inner

END920000092US1

2 of 34

S/N 09/813,911

18 connection to said outer connection for selectively
19 receiving [[or]] and sending said communication double
20 nested on said outer connection to allow subsequent
21 traffic to be correctly processed by said inner
22 connection, then by said outer connection, at both ends
23 of both connections and thereby enabling outbound
24 traffic between respective nodes selectively to flow
25 inside said outer tunnel and not said inner tunnel, in
26 said inner tunnel and said outer tunnel, and in neither
27 tunnel.

1 2. [Canceled]

1 3. [Canceled]

1 4. [Currently amended] The method of ~~claim 3~~ claim 1,
2 further comprising the step of using Layer 2 Tunnel Protocol
3 (L2TP) to tunnel packets across said communication network.

1 5. [Currently amended] Method for operating an enterprise

END920000092US1

3 of 34

S/N 09/813,911

2 gateway node to a plurality of nodes in a communication
3 network in which nested connections establish an inner
4 tunnel within an outer tunnel including an inner connection
5 and an outer connection having at least one coincident
6 endpoint residing on a said gateway node, comprising the
7 steps of:

8 receiving at said gateway node from a remote client
9 node a request to establish an outer connection;

10 receiving at said gateway over said outer connection a
11 request to establish, and thereupon negotiating
12 parameters establishing, a secure inner connection
13 using Internet key exchange (IKE) negotiations for
14 establishing an agreed upon encryption algorithm and
15 key generation and further including establishing a
16 local coincident endpoint of said inner and outer
17 connections at said gateway;

18 responsive to outbound or inbound traffic on said inner
19 connection, establishing links to said outer connection
20 for communicating said traffic double nested on said
21 outer connection to allow subsequent traffic to be
22 correctly processed by said inner connection, then by

END920000092US1

4 of 34

S/N 09/813,911

23 said outer connection, at both ends of both connections
24 and thereby enabling outbound traffic between
25 respective nodes selectively to flow inside said outer
26 tunnel and not said inner tunnel, in said inner tunnel
27 and said outer tunnel, and in neither tunnel.

28 6. [Canceled]

1 7. [Original] The method of claim 5, further comprising
2 the step of:

3 tunneling packets across said communication network
4 using Layer 2 Tunnel Protocol (L2TP).

1 8. [Currently amended] A method for operating a first one
2 of a plurality of nodes in a communications network in which
3 nested connections establish an inner tunnel within an outer
4 tunnel including an inner connection and an outer connection
5 having at least one coincident endpoint residing on said
6 first node, comprising the steps of:

END920000092US1

5 of 34

S/N 09/813,911

7 establishing at said first node a coincident endpoint
8 for an outer connection and an inner connection with at
9 least one second node in said network for setting up a
10 tunnel within a tunnel between said first and second
11 nodes and executing Internet key exchange (IKE)
12 negotiations for establishing an agreed upon encryption
13 algorithm and key generation;

14 responsive to starting communication of traffic over
15 said connections, establishing a link from said inner
16 connection to said outer connection including
17 establishing a local coincident endpoint of said inner
18 and outer connections at said first node; and

19 responsive to said links, selectively encapsulating
20 said traffic to said outer connection for transfer to
21 said second node [[or]] and decapsulating said traffic
22 from said outer connection followed by decapsulating
23 said traffic from said inner connection for receipt at
24 said first node.

1 9. [Original] The method of claim 8, said inner
2 connection being a secure connection.

END920000092US1

6 of 34

S/N 09/813,911

1 10. [Original] The method of claim 8, further comprising
2 the step of:

3 tunneling packets across said communication network
4 using Layer 2 Tunnel Protocol (L2TP).

1 11. [Currently amended] Method for nesting connections in
2 a tunnel within a tunnel having at least one coincident
3 endpoint between a plurality of nodes in a communication
4 network, said nodes including a client, ~~and internet~~ an
5 Internet service provider (ISP), an enterprise gateway, and
6 an internal network, comprising the steps of:

7 operating said client node to call said ISP node;

8 operating said ISP node to start an outer connection
9 with respect to said gateway node and to return an IP
10 address to said client node;

11 operating said client node to send to said gateway node
12 over said outer connection a request to establish a

END920000092US1

7 of 34

S/N 09/813,911

13 secure nested inner connection;

14 operating said client node and said gateway node to
15 negotiate over said outer connection parameters
16 defining said secure nested inner connection resulting
17 from Internet key exchange (IKE) negotiations for
18 establishing an agreed upon encryption algorithm and
19 key generation, and saving said parameters at said
20 gateway node; and thereafter

21 operating said client node to start said inner
22 connection;

23 operating said ISP node to decapsulate said outer
24 connection;

25 operating said client node to decapsulate said inner
26 connection; and

27 operating said gateway node to recognize the start of
28 said inner connection and to link said inner connection
29 to said outer connection to allow subsequent traffic to
30 be correctly processed by said inner connection, then
31 by said outer connection, at both ends of both

END920000092US1

8 of 34

S/N 09/813,911

32 connections, and sending outbound traffic in said inner
33 connection double nested in said outer connection.

1 12. [Canceled]

 13. [Canceled]

1 14. [Original] The method of claim 13, further comprising
2 the step of:

3 tunneling packets across said communication network
4 using Layer 2 Tunnel Protocol (L2TP).

1 15. [Currently amended] System for nesting connections
2 between a plurality of nodes in a communication network in
3 which nested connections establish a tunnel within a tunnel
4 including an inner connection and an outer connection having
5 at least one coincident endpoint residing on a same node,
6 comprising:

END920000092US1

9 of 34

S/N 09/813,911

7 a first node on an outer connection for receiving a
8 request from a second node to establish a coincident
9 endpoint for nesting an inner connection within said
10 outer connection including executing Internet key
11 exchange (IKE) negotiations for establishing an agreed
12 upon encryption algorithm and key generation;

13 said first and second nodes negotiating over said outer
14 connection parameters defining said inner connection;
15 and thereafter

16 said first node being responsive to communication
17 occurring on said inner connection for linking to said
18 outer connection for selectively receiving or sending
19 said communication double nested on said outer
20 connection to allow subsequent traffic to be correctly
21 processed by said inner connection, then by said outer
22 connection, at both ends of both connections;

23 thereby enabling outbound traffic between respective
24 nodes selectively to flow inside said outer tunnel and
25 not said inner tunnel, in said inner tunnel and said
26 outer tunnel, and in neither tunnel.

END920000092US1

10 of 34

S/N 09/813,911

1 16. [Original] The system of claim 15, said inner
2 connection being a secure connection.

1 17. [Original] The system of claim 16, said inner
2 connection being an IPsec connection.

1 18. [Original] The system of claim 17, further comprising
2 a Layer 2 Tunnel Protocol (L2TP) connection for tunneling
3 packets across said communication network.

1 19. [Currently amended] A program storage device readable
2 by a machine, tangibly embodying a program of instructions
3 executable by a machine to perform method steps for nesting
4 connections between a plurality of nodes in a communication
5 network in which nested connections establish a tunnel
6 within a tunnel including an inner connection and an outer
7 connection having at least one coincident endpoint residing
8 on a same node, said method steps comprising:

9 receiving at a first node on an outer connection a
10 request from a second node to establish a coincident

END920000092US1

11 of 34

S/N 09/813,911

11 endpoint for nesting an inner connection within said
12 outer connection;

13 negotiating over said outer connection parameters
14 defining said inner connection resulting from Internet
15 key exchange (IKE) negotiations for establishing an
16 agreed upon encryption algorithm and key generation;
17 and thereafter

18 responsive to communication occurring on said inner
19 connection, at said first node linking to said outer
20 connection for selectively receiving or sending said
21 communication double nested on said outer connection to
22 allow subsequent traffic to be correctly processed by
23 said inner connection, then by said outer connection,
24 at both ends of both connections.

1 20. [Currently amended] A program storage device readable
2 by a machine, tangibly embodying a program of instructions
3 executable by a machine to perform method steps for
4 operating an enterprise gateway in a communications network
5 in which nested connections establish a tunnel within a
6 tunnel including an inner connection and an outer connection

END920000092US1

12 of 34

S/N 09/813,911

7 having at least one coincident endpoint residing on a same
8 node, said method steps comprising:

9 receiving at said gateway from a remote client a
10 request to establish an outer connection;

11 receiving at said gateway over said outer connection a
12 request to establish, and thereupon negotiating
13 parameters including executing Internet key exchange
14 (IKE) negotiations for establishing an agreed upon
15 encryption algorithm and key generation for
16 establishing, a secure inner connection;

17 responsive to outbound or inbound traffic on said inner
18 connection, establishing links to said outer connection
19 for communicating said traffic double nested on said
20 outer connection to allow subsequent traffic to be
21 correctly processed by said inner connection, then by
22 said outer connection, at both ends of both connections
23 thereby enabling outbound traffic between respective
24 nodes selectively to flow inside said outer tunnel and
25 not said inner tunnel, in said inner tunnel and said
26 outer tunnel, and in neither tunnel.

END920000092US1

13 of 34

S/N 09/813,911

1 21. [Currently amended] A program storage device readable
2 by a machine, tangibly embodying a program of instructions
3 executable by a machine to perform method steps for
4 operating a first one of a plurality of nodes in a
5 communications network in which nested connections establish
6 a tunnel within a tunnel including an inner connection and
7 an outer connection having at least one coincident endpoint
8 residing on a same node, comprising the steps of:

9 establishing at said first node a coincident endpoint
10 for an outer connection and an inner connection with at
11 least one second node in said network;

12 responsive to starting communication of traffic over
13 said connections, establishing a link from said inner
14 connection to said outer connection including executing
15 Internet key exchange (IKE) negotiations for
16 establishing an agreed upon encryption algorithm and
17 key generation; and

18 responsive to said links, selectively encapsulating
19 said traffic to said outer connection for transfer to
20 said second node or decapsulating said traffic from
21 said outer connection for receipt at said first node to

END920000092US1

14 of 34

S/N 09/813,911

22 allow subsequent traffic to be correctly processed by
23 said inner connection, then by said outer connection,
24 at both ends of both connections.

1 22. [Currently amended] A computer program product ~~or~~
2 ~~computer program element~~ for nesting connections between a
3 plurality of nodes in a communication network in which
4 nested connections establish a tunnel within a tunnel
5 including an inner connection and an outer connection having
6 at least one coincident endpoint residing on a same node,
7 ~~according to steps~~ said computer program product comprising:

8 a digital recording medium;

9 first program instructions for receiving at a first
10 node on an outer connection a request from a second
11 node to establish a coincident endpoint for nesting an
12 inner connection within said outer connection;

13 second program instructions for negotiating over said
14 outer connection parameters defining said inner
15 connection resulting from Internet key exchange (IKE)
16 negotiations for establishing an agreed upon encryption

END920000092US1

15 of 34

S/N 09/813,911

17 algorithm and key generation; and thereafter

18 third program instructions, responsive to communication
19 occurring on said inner connection, at said first node
20 linking to said outer connection for selectively
21 receiving or sending said communication double nested
22 on said outer connection to allow subsequent traffic to
23 be correctly processed by said inner connection, then
24 by said outer connection, at both ends of both
25 connections; thereby enabling outbound traffic between
26 respective nodes selectively to flow inside said outer
27 tunnel and not said inner tunnel, in said inner tunnel
28 and said outer tunnel, and in neither tunnel; and
29 wherein

30 said first, second and third program instructions are
31 recorded on said digital recording medium.

1 23. [Currently amended] A computer program product or
2 ~~computer program element for perform method steps for~~
3 ~~operating an enterprise gateway~~ node to a network in which
4 nested connections establish a tunnel within a tunnel
5 including an inner connection and an outer connection having

END920000092US1

16 of 34

S/N 09/813,911

6 at least one coincident endpoint residing on said gateway
7 node, according to method steps said computer program
8 product comprising:

9 a digital recording medium;

10 first program instructions for receiving at said
11 gateway from a remote client a request to establish an
12 outer connection;

13 second program instructions for receiving at said
14 gateway over said outer connection a request to
15 establish, and thereupon negotiating parameters
16 establishing, a secure inner connection resulting from
17 Internet key exchange (IKE) negotiations for
18 establishing an agreed upon encryption algorithm and
19 key generation;

20 third program instructions, responsive to outbound or
21 inbound traffic on said inner connection, for
22 establishing links to said outer connection for
23 communicating said traffic double nested on said outer
24 connection to allow subsequent traffic to be correctly
25 processed by said inner connection, then by said outer

END920000092US1

17 of 34

S/N 09/813,911

26 connection, at both ends of both connections; and
27 wherein

28 said first, second, and third program instructions are
29 recorded on said digital recording medium.

1 24. [Currently amended] A computer program product or
2 ~~computer program element~~ for operating a first one of a
3 plurality of nodes in a communications network in which
4 nested connections establish a tunnel within a tunnel
5 including an inner connection and an outer connection having
6 at least one coincident endpoint residing on a same node
7 ~~according to method steps~~ said computer program product
8 comprising:

9 a magnetic recording medium;

10 first program instructions for establishing at said
11 first node a coincident endpoint for an outer
12 connection and an inner connection with at least one
13 second node in said network;

14 second program instructions, responsive to starting

END920000092US1

18 of 34

S/N 09/813,911

15 communication of traffic over said connections, for
16 executing Internet key exchange (IKE) negotiations for
17 establishing an agreed upon encryption algorithm and
18 key generation and establishing a link from said inner
19 connection to said outer connection; and

20 third program instructions, responsive to said links,
21 for selectively encapsulating said traffic to said
22 outer connection for transfer to said second node or
23 decapsulating said traffic from said outer connection
24 for receipt at said first node to allow subsequent
25 traffic to be correctly processed by said inner
26 connection, then by said outer connection, at both ends
27 of both connections; and wherein

28 said first, second, and third program instructions are
29 recorded on said medium.

END920000092US1

19 of 34

S/N 09/813,911